



Microsoft Azure Administrator

SECOND EDITION

Exam Ref **AZ-104**

Charles Pluta

FREE SAMPLE CHAPTER |



Exam Ref AZ-104 Microsoft Azure Administrator

Second Edition

Charles Pluta

Exam Ref AZ-104 Microsoft Azure Administrator, Second Edition

Published with the authorization of Microsoft Corporation by: Pearson Education, Inc.

Copyright © 2025 by Pearson Education, Inc.
Hoboken, New Jersey

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/permissions.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-13-834593-8

ISBN-10: 0-13-834593-7

Library of Congress Control Number: 2024935895

\$PrintCode

TRADEMARKS

Microsoft and the trademarks listed at <http://www.microsoft.com> on the "Trademarks" webpage are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

WARNING AND DISCLAIMER

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author, the publisher, and Microsoft Corporation shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the programs accompanying it.

SPECIAL SALES

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

CREDITS

EDITOR-IN-CHIEF
Brett Bartow

EXECUTIVE EDITOR
Loretta Yates

ASSOCIATE EDITOR
Shourav Bose

DEVELOPMENT EDITOR
Songlin Qiu

MANAGING EDITOR
Sandra Schroeder

SENIOR PROJECT EDITOR
Tracey Croom

COPY EDITOR
Brie Gyncild

INDEXER
Timothy Wright

PROOFREADER
Charlotte Kughen

TECHNICAL EDITOR
Jim Cheshire

EDITORIAL ASSISTANT
Cindy Teeters

COVER DESIGNER
Twist Creative, Seattle

COMPOSITOR
codeMantra

GRAPHICS
codeMantra

Contents at a glance

	<i>Acknowledgments</i>	<i>x</i>
	<i>About the author</i>	<i>x</i>
	<i>Introduction</i>	<i>xi</i>
CHAPTER 1	Manage Azure identities and governance	1
CHAPTER 2	Implement and manage storage	65
CHAPTER 3	Deploy and manage Azure compute resources	123
CHAPTER 4	Configure and manage virtual networking	215
CHAPTER 5	Monitor and back up Azure resources	291
CHAPTER 6	Exam Ref AZ-104 Microsoft Azure Administrator exam updates	357
	<i>Index</i>	<i>362</i>

Contents

Introduction	xi
<i>Organization of this book</i>	<i>xi</i>
<i>Preparing for the exam</i>	<i>xi</i>
<i>Microsoft certifications</i>	<i>xii</i>
<i>Access the exam updates chapter and online references</i>	<i>xii</i>
<i>Errata, updates & book support</i>	<i>xiii</i>
<i>Stay in touch</i>	<i>xiii</i>
 Chapter 1 Manage Azure identities and governance	 1
Skill 1.1: Manage Microsoft Entra users and groups.....	2
Create users and groups	3
Manage user and group properties	6
Manage licenses in Microsoft Entra ID	10
Manage external users	10
Configure Microsoft Entra Join	12
Configure self-service password reset	14
Skill 1.2: Manage access to Azure resources	16
Understand how RBAC works	16
Create a custom role	20
Interpret access assignments	25
Manage multiple directories	28
Skill 1.3: Manage Azure subscriptions and governance	29
Configure Azure policies	31
Configure resource locks	38
Apply and manage tags on resources	40
Manage resource groups	41
Manage Azure subscriptions	48
Configure management groups	50
Configure cost management	53

Chapter summary	61
Thought experiment.....	63
Thought experiment answers	63
Chapter 2 Implement and manage storage	65
Skill 2.1: Configure access to storage	65
Create and configure storage accounts	66
Configure Azure Storage firewalls and virtual networks	74
Create and use shared access signature (SAS) tokens	78
Configure stored access policies	81
Manage access keys	83
Configure identity-based access	84
Skill 2.2: Configure and manage storage accounts	89
Configure Azure storage redundancy	89
Configure object replication	91
Configure storage account encryption	95
Manage data using Azure Storage Explorer	95
Manage data by using AzCopy	99
Skill 2.3: Configure Azure Files and Azure Blob Storage	101
Create and configure a file share in Azure Storage	102
Configure Azure Blob Storage	106
Configure storage tiers	110
Configure soft delete, versioning, and snapshots	113
Configure blob lifecycle management	117
Chapter summary	120
Thought experiment.....	121
Thought experiment answers	122
Chapter 3 Deploy and manage Azure compute resources	123
Skill 3.1: Automate deployment of resources	124
Interpret an Azure Resource Manager template	124
Modify an existing ARM template	131
Deploy resources from a template	133

Chapter summary	353
Thought experiment.....	354
Thought experiment answers	355
Chapter 6 Exam Ref AZ-104 Microsoft Azure	
Administrator exam updates	357
The purpose of this chapter	357
About possible exam updates	358
Impact on you and your study plan	358
News and commentary about the exam objective updates.....	358
Updated technical content.....	359
Objective mapping	359
<i>Index</i>	362

Acknowledgments

I would like to acknowledge my wife, Jennifer, who has supported the unusual hours for projects such as this for over a decade now. I would also like to acknowledge my best friends and colleagues who allow me to bounce ideas off them, provide guidance to them, and share laughs with them: Elias Mereb, Joshua Waddell, Ed Gale, and Aaron Lines. Finally, I have to thank my manager, Julia Nathan, who has been an exemplary coach and role model and continues to support my work on projects such as this book.

About the Author

CHARLES PLUTA is a technical consultant and Microsoft Certified Trainer (MCT) who has authored several certification exams, lab guides, and learner guides for various technology vendors. As a technical consultant, Charles has assisted small, medium, and large organizations by deploying and maintaining their IT infrastructure. He is also a speaker, a staff member, or a trainer at several large annual industry conferences. Charles has a degree in Computer Networking, and holds over 15 industry certifications. He makes a point to leave the United States to travel to a different country every year. When not working or traveling, he plays pool in Augusta, Georgia.

Introduction

Some books take a very low-level approach, teaching you how to use individual classes and accomplish fine-grained tasks. Like the Microsoft AZ-104 certification exam, this book takes a high-level approach, building on your foundational knowledge of Microsoft Azure and common administrative actions to take in an Azure environment. We provide walk-throughs using the Azure portal; however, the exam might also include questions that use PowerShell or the Azure Command Line Interface (CLI) to perform the same task. You might encounter questions on the exam focused on these additional areas that are not specifically included in this *Exam Ref*.

This book covers every major topic area found on the exam, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions, and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book that you do not feel completely comfortable with, use the “Need more review?” links you’ll find in the text to find more information and take the time to research and study the topic.

Organization of this book

This book is organized by the “Skills measured” list published for the exam. The “Skills measured” list is available for each exam on the Microsoft Learn website: microsoft.com/learn. Each chapter in this book corresponds to a major topic area in the list, and the technical tasks in each topic area determine a chapter’s organization. If an exam covers six major topic areas, for example, the book will contain six chapters.

Preparing for the exam

Microsoft certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. This book is *not* designed to teach you new skills.

We recommend that you augment your exam preparation plan by using a combination of available study materials and courses. For example, you might use the *Exam Ref* and another study guide for your at-home preparation and take a Microsoft Official Curriculum course for the classroom experience. Choose the combination that you think works best for you. Learn more about available classroom training, online courses, and live events at microsoft.com/learn.

Note that this *Exam Ref* is based on publicly available information about the exam and the author's experience. To safeguard the integrity of the exam, authors do not have access to the live exam.

Microsoft certifications

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies both on-premises and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

MORE INFO ALL MICROSOFT CERTIFICATIONS

For information about Microsoft certifications, including a full list of available certifications, go to microsoft.com/learn.

Access the exam updates chapter and online references

The final chapter of this book, "AZ-104 Azure Administrator exam updates," will be used to provide information about new content per new exam topics, content that has been removed from the exam objectives, and revised mapping of exam objectives to chapter content. The chapter will be made available from the link at the end of this section as exam updates are released.

Throughout this book are addresses to webpages that the author has recommended you visit for more information. We've compiled them into a single list that readers of the print edition can refer to while they read.

The URLs are organized by chapter and heading. Every time you come across a URL in the book, find the hyperlink in the list to go directly to the webpage.

Download the exam updates chapter and the URL list at MicrosoftPressStore.com/ERAZ1042e/downloads.

Errata, updates & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at

MicrosoftPressStore.com/ERAZ1042e/errata

If you discover an error that is not already listed, please submit it to us at the same page.

For additional book support and information, please visit *MicrosoftPressStore.com/Support*.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *support.microsoft.com*.

Stay in touch

Let's keep the conversation going! We're on X/Twitter: *twitter.com/MicrosoftPress*.

Implement and manage storage

Implementing and managing storage is one of the most important aspects of building or deploying a new solution using Azure. There are several services and features available for use, and each has its own place. Azure Storage is the underlying storage for most of the services in Azure. It provides service for the storage and retrieval of blobs and files, and it has services that are available for storing large volumes of data through tables. Azure Storage includes a fast and reliable messaging service for application developers with queues. This chapter reviews how to implement and manage storage with an emphasis on Azure storage accounts.

Skills covered in this chapter:

- Skill 2.1 Configure access to storage
- Skill 2.2: Configure and manage storage accounts
- Skill 2.3: Configure Azure Files and Azure Blob Storage

NOTE MICROSOFT EXAM OBJECTIVES

The sections in this chapter align with the objectives that are listed in the AZ-104 study guide from Microsoft. However, the sections are presented in an order that is designed to help you learn and do not directly match the order that is presented in the study guide. On the exam, questions will appear from different sections in a random order. For the full list of objectives, visit <https://learn.microsoft.com/en-us/credentials/certifications/resources/study-guides/az-104>.

Skill 2.1: Configure access to storage

An Azure storage account is a resource that you create that is used to store data objects such as blobs, files, queues, tables, and disks. Data in an Azure storage account is durable and highly available, secure, massively scalable, and accessible from anywhere in the world over HTTP or HTTPS.

This skill covers how to:

- Create and configure storage accounts
- Configure Azure Storage firewalls and virtual networks
- Create and use shared access signature (SAS) tokens
- Configure stored access policies
- Manage access keys
- Configure identity-based access

Create and configure storage accounts

Azure storage accounts provide a cloud-based storage service that is highly scalable, available, performant, and durable. Within each storage account, a number of separate storage services are provided:

- **Blobs** Provides a highly scalable service for storing arbitrary data objects such as text or binary data.
- **Tables** Provides a NoSQL-style store for storing structured data. Unlike a relational database, tables in Azure Storage do not require a fixed schema, so different entries in the same table can have different fields.
- **Queues** Provides reliable message queueing between application components.
- **Files** Provides managed file shares that can be used by Azure VMs or on-premises servers.
- **Disks** Provides a persistent storage volume for Azure VM that can be attached as a virtual hard disk.

There are three types of storage blobs: block blobs, append blobs, and page blobs. Page blobs are generally used to store VHD files when deploying unmanaged disks. (Unmanaged disks are an older disk storage technology for Azure virtual machines. Managed disks are recommended for new deployments.)

When creating a storage account, there are several options that must be set: Performance Tier, Account Kind, Replication Option, and Access Tier. There are some interactions between these settings. For example, only the Standard performance tier allows you to choose the access tier. The following sections describe each of these settings. We then describe how to create storage accounts using the Azure portal, PowerShell, and Azure CLI.

Storage account names

When you name an Azure storage account, you need to remember these points:

- The storage account name must be globally unique across all existing storage account names in Azure.
- The name must be between 3 and 24 characters and can contain only lowercase letters and numbers.

Performance tiers

When creating a storage account, you must choose between the Standard and Premium performance tiers. This setting cannot be changed later.

- **Standard** This tier supports all storage services: blobs, tables, files, queues, and unmanaged Azure virtual machine disks. It uses magnetic disks to provide cost-efficient and reliable storage.
- **Premium** This tier is designed to support workloads with greater demands on I/O and is backed by high-performance SSD disks. Premium storage accounts support block blobs, page blobs, and file shares.

Account types

There are three possible storage account types for the Standard tier: StorageV2 (General-Purpose V2), Storage (General-Purpose V1), and BlobStorage. There are four possible storage account types for the Premium tier: StorageV2 (General-Purpose V2), Storage (General-Purpose V1), BlockBlobStorage, and FileStorage. Table 2-1 shows the features for each kind of account. Key points to remember are

- The Blob Storage account is a specialized storage account used to store Block Blobs and Append Blobs. You can't store Page Blobs in these accounts; therefore, you can't use them for unmanaged disks.
- Only General-Purpose V2 and Blob Storage accounts support the Hot, Cool, and Archive access tiers.

General-Purpose V1 and Blob Storage accounts can both be upgraded to a General-Purpose V2 account. This operation is irreversible. No other changes to the account kind are supported.

NOTE LEGACY STORAGE ACCOUNT TYPES

Standard General-Purpose V1 and standard Blob Storage accounts are considered legacy storage accounts, and they can be deployed but are not recommended by Microsoft. You can find more information about legacy storage account types at <https://learn.microsoft.com/en-us/azure/storage/common/storage-account-overview#legacy-storage-account-types>.

TABLE 2-1 Storage account types and their supported features

	General-Purpose V2	General-Purpose V1	Blob Storage	Block Blob Storage	File Storage
Services supported	Blob, File, Queue, Table	Blob, File, Queue, Table	Blob (Block Blobs and Append Blobs only)	Blob (Block Blobs and Append Blobs only)	File only
Unmanaged Disk (Page Blob) support	Yes	Yes	No	No	No

	General-Purpose V2	General-Purpose V1	Blob Storage	Block Blob Storage	File Storage
Supported Performance Tiers	Standard Premium	Standard Premium	Standard	Premium	Premium
Supported Access Tiers	Hot, Cool, Archive	N/A	Hot, Cool, Archive	N/A	N/A
Replication Options	LRS, ZRS, GRS, RA-GRS, GZRS, RA-GZRS	LRS, GRS, RA-GRS	LRS, GRS, RA-GRS	LRS, ZRS	LRS, ZRS

Replication options

When you create a storage account, you can also specify how your data will be replicated for redundancy and resistance to failure. There are four options, as described in Table 2-2.

TABLE 2-2 Storage account replication options

Replication Type	Description
Locally redundant storage (LRS)	Makes three synchronous copies of your data within a single datacenter. Available for General-Purpose or Blob Storage accounts, at both the Standard and Premium Performance tiers.
Zone redundant storage (ZRS)	Makes three synchronous copies to three separate availability zones within a single region. Available for General-Purpose V2 storage accounts only, at the Standard Performance tier only. Also available for Block Blob Storage and File Storage accounts.
Geographically redundant storage (GRS)	This is the same as LRS (three local synchronous copies), plus three additional asynchronous copies to a second Azure region hundreds of miles away from the primary region. Data replication typically occurs within 15 minutes, although no SLA is provided. Available for General-Purpose or Blob Storage accounts, at the Standard Performance tier only.
Read access geographically redundant storage (RA-GRS)	This has the same capabilities as GRS, plus you have read-only access to the data in the secondary data center. Available for General-Purpose or Blob Storage accounts, at the Standard Performance tier only.
Geographically zone redundant storage (GZRS)	This is the same as ZRS (three synchronous copies across multiple availability zones in the selected region), plus three additional asynchronous copies to a different Azure region hundreds of miles away from the primary region. Data replication typically occurs within 15 minutes, although no SLA is provided. Available for General-Purpose v2 storage accounts only, at the Standard Performance tier only.
Read access geographically zone redundant storage (RA-GZRS)	This has the same capabilities as GZRS, plus you have read-only access to the data in the secondary data center. Available for General-Purpose V2 storage accounts only, at the Standard Performance tier only.

NOTE REPLICATION OPTIONS

These replication options control the level of durability and availability of the storage account. When the entire datacenter is unavailable, LRS would incur an outage. If the primary region is unavailable, both the LRS and ZRS options would incur an outage, but the GRS and GZRS options would still provide the secondary region that takes care of the requests during the outage. However, not all the replication options are available in all regions. You can find supported regions with these replication options at <https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy>.

NOTE SPECIFYING REPLICATION AND PERFORMANCE TIER SETTINGS

When creating a storage account via the Azure portal, the replication and performance tier options are specified using separate settings. When creating an account using Azure PowerShell, the Azure CLI, or via a template, these settings are combined within the SKU setting.

For example, to specify a Standard storage account using locally redundant storage using the Azure CLI, use `--sku Standard_LRS`.

Access tiers

Azure Blob Storage supports four access tiers: Hot, Cool, Cold, and Archive. Each represents a trade-off of availability and cost. There is no trade-off on the durability (probability of data loss), which is defined by the SKU and replication, not the access tier.

NOTE BLOB STORAGE ONLY

Access tiers apply to Block Blob Storage only. They do not apply to other storage services, including append or page Blob Storage.

The tiers are as follows:

- **Hot** This access tier is used to store frequently accessed objects. Relative to other tiers, data access costs are low while storage costs are higher.
- **Cool** This access tier is used to store large amounts of data that is not accessed frequently and that is stored for at least 30 days. The availability SLA can vary depending on the replication model selected. Relative to the Hot tier, data access costs are higher and storage costs are lower.
- **Cold** This access tier is used for data that is rarely accessed or modified but needs to be accessible without delay. Data in this tier should be stored for at least 90 days. The Cold tier pricing model has lower storage capacity costs but higher access costs compared to cool and hot tiers.
- **Archive** This access tier is used to archive data for long-term storage that is accessed rarely, can tolerate several hours of retrieval latency, and will remain in the Archive

tier for at least 180 days. This tier is the most cost-effective option for storing data, but accessing that data is more expensive than accessing data in other tiers. Blob rehydration might take up to 15 hours before the blob is accessible.

New blobs will default to the access tier that is set at the storage account level, though you can override that at the blob level by setting a different access tier, including the archive tier.

NOTE ARCHIVE TIER SUPPORTABILITY

Currently, the Archive tier is not supported for ZRS, GZRS, or RA-GZRS accounts.

Create an Azure storage account

To create a storage account using the Azure portal, type **storage accounts** in the search box. On the Storage Accounts blade, click Create to open the Create A Storage Account blade (see Figure 2-1). You must choose a unique name for the storage account. Storage account names must be globally unique and may only contain lowercase characters and digits. Select the Azure region (Location), the performance tier, and replication mode for the account. The blade adjusts based on the settings you choose so that you cannot select an unsupported feature combination.

Home > Storage accounts >

Create a storage account ...

Basics Advanced Networking Data protection Encryption Tags Review

Subscription * Azure Pass - Sponsorship

Resource group * az104-rg1
[Create new](#)

Instance details

Storage account name ⓘ * az104demo123

Region ⓘ * (US) East US
[Deploy to an edge zone](#)

Performance ⓘ *
☒ **Standard:** Recommended for most scenarios (general-purpose v2 account)
☐ **Premium:** Recommended for scenarios that require low latency.

Redundancy ⓘ * Geo-redundant storage (GRS)
☒ Make read access to data available in the event of regional unavailability.

[Review](#) [< Previous](#) [Next : Advanced >](#)

FIGURE 2-1 Creating an Azure storage account using the Azure portal

The Advanced tab of the Create A Storage Account blade is shown in Figure 2-2. This tab defines additional security settings, hierarchical namespace support, and access protocols.

The screenshot shows the 'Create a storage account' blade in the Azure portal, specifically the 'Advanced' tab. The breadcrumb navigation at the top reads 'Home > Storage accounts >'. The main heading is 'Create a storage account' followed by a three-dot menu icon. Below the heading is a horizontal tab bar with the following tabs: 'Basics', 'Advanced' (which is selected and underlined), 'Networking', 'Data protection', 'Encryption', 'Tags', and 'Review'. The 'Security' section is active, with the sub-header 'Security' and a description: 'Configure security settings that impact your storage account.' There are six settings listed: 1. 'Require secure transfer for REST API operations' with a blue checkmark icon. 2. 'Allow enabling anonymous access on individual containers' with an unchecked checkbox. 3. 'Enable storage account key access' with a blue checkmark icon. 4. 'Default to Microsoft Entra authorization in the Azure portal' with an unchecked checkbox. 5. 'Minimum TLS version' with a dropdown menu showing 'Version 1.2'. 6. 'Permitted scope for copy operations (preview)' with a dropdown menu showing 'From any storage account'. Below these settings is the 'Hierarchical Namespace' section, which is currently empty. At the bottom of the blade, there are three buttons: a blue 'Review' button, a '< Previous' button, and a 'Next : Networking >' button.

FIGURE 2-2 The advanced settings that can be set when creating an Azure storage account using the portal

The Networking tab of the Create A Storage Account blade is shown in Figure 2-3. On this tab, choose to maintain storage account access either publicly by choosing Enable Public Access From All Networks or privately by choosing Disable Public Access And Use Private Access.

Create a storage account ...

Basics Advanced **Networking** Data protection Encryption Tags Review

Network connectivity

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Network access *

- ☒ Enable public access from all networks
- ☐ Enable public access from selected virtual networks and IP addresses
- ☐ Disable public access and use private access
- i** Enabling public access from all networks might make this resource available publicly. Unless public access is required, we recommend using a more restricted access type. [Learn more](#)

Network routing

Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.

Routing preference ⓘ *

- ☒ Microsoft network routing

[Review](#)

[< Previous](#)

[Next : Data protection >](#)

FIGURE 2-3 The networking properties that can be set when creating an Azure storage account using the portal

The Data Protection tab provides options for configuring the recovery, tracking, and access control of the storage account. This includes soft delete options, retention periods, blob versioning, and version-level immutability support. Figure 2-4 shows the Data Protection tab.

The Encryption tab provides options for configuring the encryption type, support for customer-managed keys, and infrastructure encryption. By default, storage accounts are encrypted using Microsoft-managed keys. However, you can configure customer-managed keys to encrypt data using your own keys. Figure 2-5 shows the Encryption tab.

Home > Storage accounts >

Create a storage account ...

Basics Advanced Networking **Data protection** Encryption Tags Review

Recovery

Protect your data from accidental or erroneous deletion or modification.

☐ Enable point-in-time restore for containers
Use point-in-time restore to restore one or more containers to an earlier state. If point-in-time restore is enabled, then versioning, change feed, and blob soft delete must also be enabled. [Learn more](#)

☒ Enable soft delete for blobs
Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. [Learn more](#)

Days to retain deleted blobs ⓘ

☒ Enable soft delete for containers
Soft delete enables you to recover containers that were previously marked for deletion. [Learn more](#)

Days to retain deleted containers ⓘ

☒ Enable soft delete for file shares
Soft delete enables you to recover file shares that were previously marked for deletion. [Learn more](#)

Days to retain deleted file shares ⓘ

[Review](#) [< Previous](#) [Next : Encryption >](#)

FIGURE 2-4 The data protection properties that can be set when creating an Azure storage account using the portal

Home > Storage accounts >

Create a storage account ...

Basics Advanced Networking Data protection **Encryption** Tags Review

Encryption type * ⓘ

☒ Microsoft-managed keys (MMK)

☐ Customer-managed keys (CMK)

Enable support for customer-managed keys ⓘ

☒ Blobs and files only

☐ All service types (blobs, files, tables, and queues)

⚠ This option cannot be changed after this storage account is created.

Enable infrastructure encryption ⓘ ☐

[Review](#) [< Previous](#) [Next : Tags >](#)

FIGURE 2-5 The encryption properties that can be set when creating an Azure storage account using the portal

NEED MORE REVIEW? CREATING A STORAGE ACCOUNT WITH POWERSHELL

You can learn more about the additional parameters at <https://learn.microsoft.com/en-us/powershell/module/az.storage/new-azstorageaccount?view=azps-11.2.0>.

NEED MORE REVIEW? CREATING A STORAGE ACCOUNT WITH THE AZURE CLI

You can learn more about the additional parameters at <https://learn.microsoft.com/en-us/cli/azure/storage/account?view=azure-cli-latest#az-storage-account-create>.

Configure Azure Storage firewalls and virtual networks

Storage accounts are managed through Azure Resource Manager. Management operations are authenticated and authorized using Microsoft Entra ID RBAC. Each storage service exposes its own endpoint used to manage the data in that storage service (blobs in Blob Storage, entities in tables, and so on). These service-specific endpoints are not exposed through Azure Resource Manager; instead, they are (by default) internet-facing endpoints.

Access to these internet-facing storage endpoints must be secured, and Azure Storage provides several ways to do so. In this section, you will review the network-level access controls: the storage firewall and service endpoints. This section also discusses Blob Storage access levels. The following sections then describe the application-level controls: shared access signatures and access keys. In later sections, you will learn about Azure Storage replication and how to leverage Microsoft Entra ID authentication for a storage account.

Storage firewall

Using the storage firewall, you can limit access to specific IP addresses or an IP address range. It applies to all storage services endpoints (blobs, tables, queues, and files). For example, by limiting access to the IP address range of your company, access from other locations will be blocked. Service endpoints are used to restrict access to specific subnets within an Azure virtual network.

To configure the storage firewall using the Azure portal, open the storage account blade and click Networking. Under Public Network Access, select Enabled From Selected Virtual Networks And IP Addresses to reveal the Firewall and Virtual Networks settings, as shown in Figure 2-6.

When accessing the storage account via the internet, use the storage firewall to specify the internet-facing source IP addresses (for example, 32.54.231.0/24, as shown in Figure 2-6) which will make the storage requests. All internet traffic is denied, except the defined IP addresses in the storage firewall. You can specify a list of either individual IPv4 addresses or IPv4 CIDR address ranges. (CIDR notation is explained in Skill 4.1 in Chapter 4, “Configure and manage virtual networking.”)

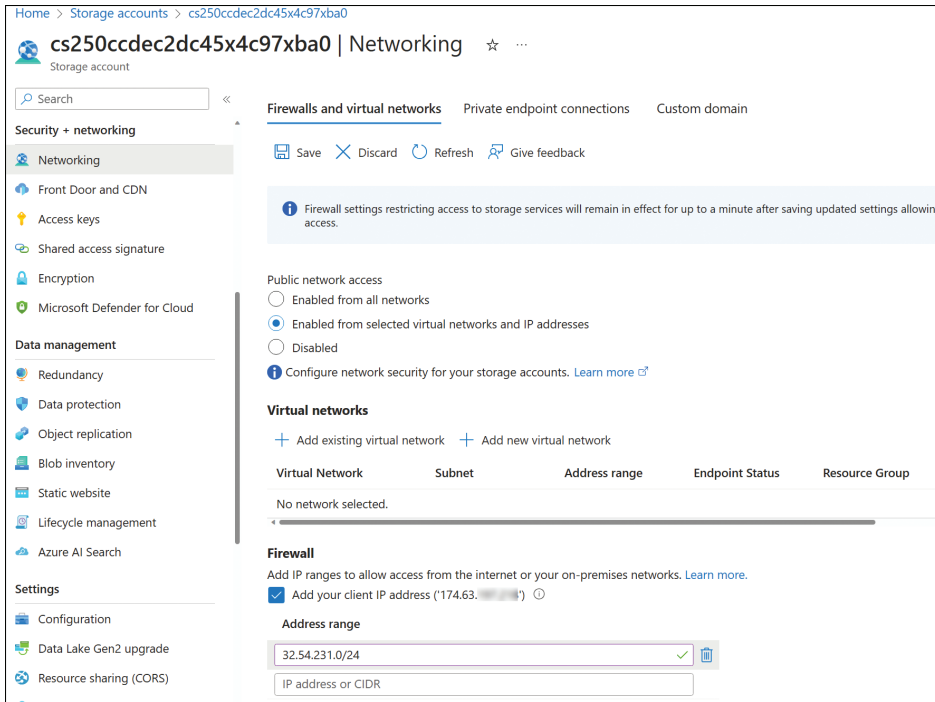


FIGURE 2-6 Configuring a storage account firewall and virtual network service endpoint access

The storage firewall includes an option to allow access from trusted Microsoft services. As an example, these services include Azure Backup, Azure Site Recovery, Azure Networking, and more. For example, it will allow access to storage for NSG flow logs if Allow Trusted Microsoft Services To Access This Account is selected. Separately, you can enable Allow Read Access To Storage Logging From Any Network or Allow Read Access To Storage Metrics From Any Network to allow read-only access to storage metrics and logs.

NOTE ADDRESS SPACE FOR A STORAGE FIREWALL

When creating a storage firewall, you must use public internet IP address space. You cannot use IPs in the private IP address space. Additionally, you cannot use /32 or /31 as a CIDR range, you must specify the individual IP addresses for individual or small ranges.

Virtual network service endpoints

In some scenarios, a storage account is only accessed from within an Azure virtual network. In this case, it is desirable from a security standpoint to block all internet access. Configuring virtual network service endpoints for your Azure storage account, you can remove access from the public internet and only allow traffic from a virtual network for improved security.

Another benefit of using service endpoints is optimized routing. Service endpoints create a direct network route from the virtual network to the storage service. If forced tunneling is

being used to force internet traffic to your on-premises network or to another network appliance, requests to Azure Storage will follow that same route. By using service endpoints, you can use a direct route to the storage account instead of the on-premises route, so no additional latency is incurred.

Configuring service endpoints requires two steps. First, to update the subnet settings, you should choose your virtual network from the Virtual Networks blade. Then select Subnets on the left under Settings. Click the subnet you plan to configure to access the subnet settings. After selecting the desired subnet, under Service Endpoints, choose Microsoft.Storage from the Services drop-down menu. This creates the route from the subnet to the storage service but does not restrict which storage account the virtual network can use. Figure 2-7 shows the subnet settings, including the service endpoint configuration.

subnet0

vnet-eus-az104

Name

subnet0

Subnet address range *

10.0.0.0/24

10.0.0.0 - 10.0.0.255 (251 + 5 Azure reserved addresses)

☐ Add IPv6 address space

NAT gateway

None

Network security group

None

Route table

None

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services

Microsoft.Storage

Service	Status
Microsoft.Storage	Succeeded

Service endpoint policies

0 selected

SUBNET DELEGATION

Save

Cancel

Give feedback

FIGURE 2-7 Configuring a subnet with a service endpoint for Azure Storage

The second step is to configure which virtual networks can access a particular storage account. From the storage account blade, click Networking. Under Public Network Access, click Enabled From Selected Virtual Networks And IP Addresses to reveal the Firewall and Virtual Network settings, as shown previously in Figure 2-1. Under Virtual Networks, select Add Existing Virtual Network to add the virtual networks and subnets that should have access to this storage account.

Blob Storage access levels

Storage accounts support an additional access control mechanism that is limited only to Blob Storage. By default, no public read access is enabled for anonymous users, and only users with rights granted through RBAC or with the storage account name and key will have access to the stored blobs. To enable anonymous user access, you must enable Allow Blob Anonymous Access (shown in Figure 2-8) and configure the container access level (shown in Figure 2-9).

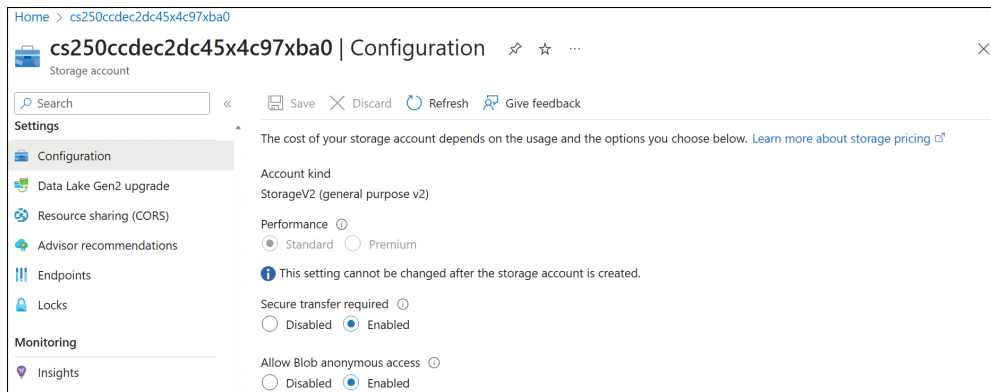


FIGURE 2-8 Storage account configuration

The anonymous access level for a container can be specified during creation, or modified after it has been created. The supported levels of blob containers are as follows:

- **Private** Only principals with permissions can access the container and its blobs. Anonymous access is denied.
- **Blob** Only blobs within the container can be accessed anonymously.
- **Container** Blobs and their containers can be accessed anonymously.

You can change the access level through the Azure portal, Azure PowerShell, Azure CLI, programmatically using the REST API, or by using Azure Storage Explorer. The access level is configured separately on each blob container.

FIGURE 2-9 Blob Storage access levels

A shared access signature token (SAS token) is a URI query string parameter that grants access to containers, blobs, queues, and/or tables. Use a SAS token to grant access to a client or service that should not have access to the entire contents of the storage account (and therefore, should not have access to the storage account keys) but still requires secure authentication. By distributing a SAS URI to these clients, you can grant them access to a specific resource, for a specified period of time, and with a specified set of permissions. SAS tokens are commonly used to read and write the data to users' storage accounts. Also, SAS tokens are widely used to copy blobs or files to another storage account.

NOTE SAS TOKENS USING HTTPS

When dealing with SAS tokens, you must use only the HTTPS protocol. Because active SAS tokens provide direct authentication to your storage account, you must use a secure connection, such as HTTPS, to distribute SAS token URIs.

Create and use shared access signature (SAS) tokens

There are a few different ways you can create a SAS token. A SAS token is a way to granularly control how a client can access data in an Azure storage account. You can also use an account-level SAS to access the account itself. You can control many things, such as what services and resources the client can access, what permission the client has, how long the token is valid for, and more.

This section examines how to create SAS tokens using various methods. The simplest way to create one is by using the Azure portal. Browse to the Azure storage account and open the Shared Access Signature blade (see Figure 2-10). You can check the services, resource types, and permissions based on specific requirements, along with the duration for the SAS token validity and the IP addresses that are providing access. Lastly, you have an option to choose which key you want to use as the signing key for this token.

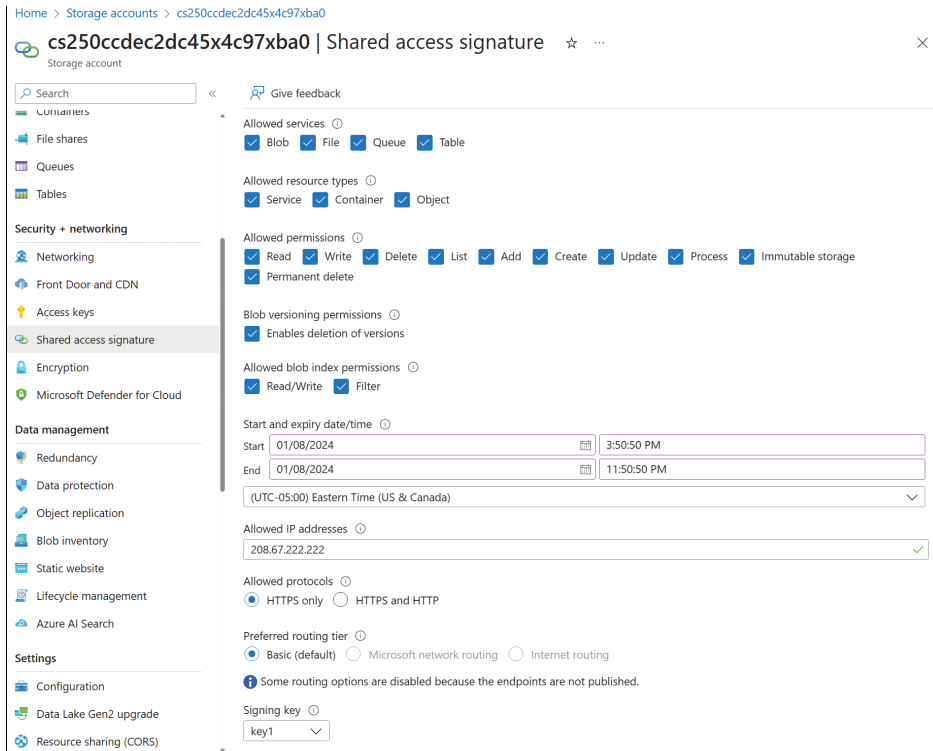


FIGURE 2-10 Creating a shared access signature using the Azure portal

Once the token is generated, it will be listed along with connection string and SAS URLs, as shown in Figure 2-11.

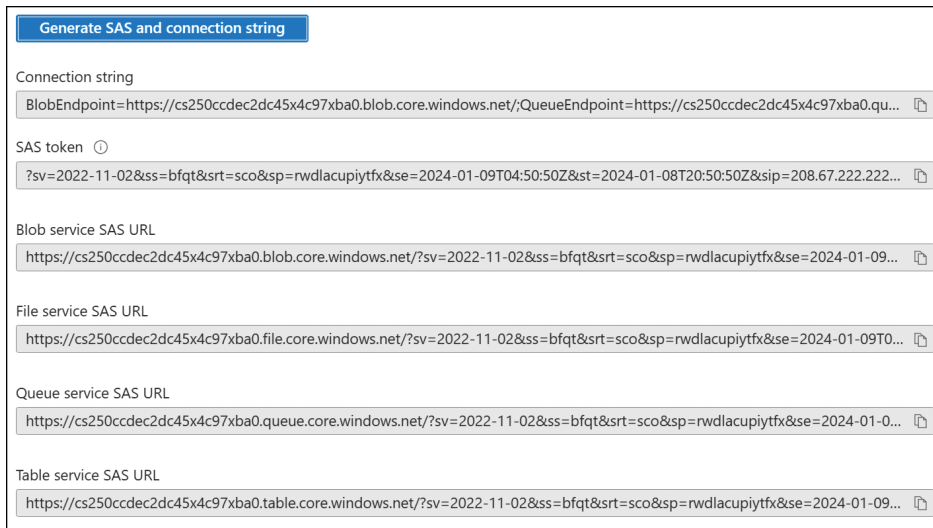


FIGURE 2-11 Generated SAS token with connection string and SAS URLs

Also, you can create SAS tokens using Storage Explorer or the command-line tools (or programmatically using the REST APIs/SDK). To create a SAS token using Storage Explorer, you need to first select the resource (storage account, container, blob, and so on) for which the SAS token needs to be created. Then right-click the resource and select Get Shared Access Signature. Figure 2-12 demonstrates how to create a SAS token using Azure Storage Explorer.

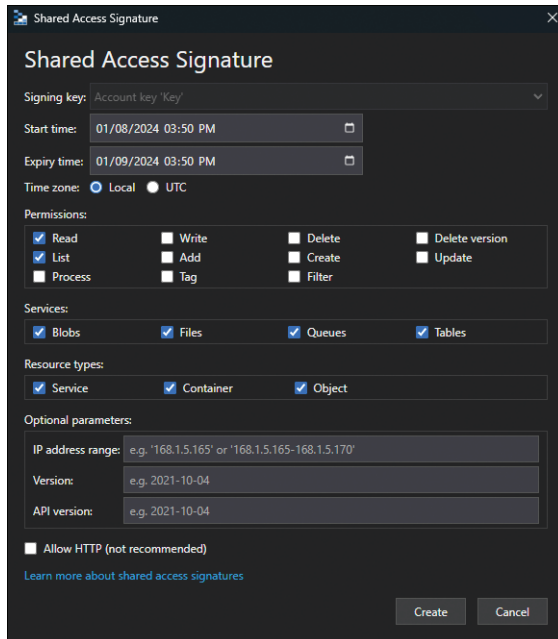


FIGURE 2-12 Creating a shared access signature using Azure Storage Explorer

NEED MORE REVIEW? AZURE STORAGE EXPLORER

Azure Storage Explorer is a free download from Microsoft that enables convenient cloud storage management from your device. Learn more about Azure Storage Explorer at <https://azure.microsoft.com/en-us/products/storage/storage-explorer/>.

Use shared access signatures

Each SAS token is a query string parameter that can be appended to the full URI of the blob or other storage resource for which the SAS token was created. Create the SAS URI by appending the SAS token to the full URI of the blob or other storage resource.

The following example shows the combination in more detail. Suppose the storage account name is examref, the blob container name is examrefcontainer, and the blob path is sample-file.png. The full URI to the blob in storage is

`https://examrefstorage.blob.core.windows.net/examrefcontainer/sample-file.png`

The combined URI with the generated SAS token is

```
https://examrefstorage.blob.core.windows.net/examrefcontainer/sample-file.png?sv=2024-01-02&ss=bfqt&srt=sco&sp=rwdl&acupx&se=2024-02-02T08:50:14Z&st=2024-01-01T00:50:14Z&spr=h  
ttps&sig=65tNhZtj2lU0tiH8HQtk7aEL9YCIpGGprZocXjiQ%2Fko%3D
```

Currently, stored access policy is not supported for account-level SAS.

NEED MORE REVIEW? ACCOUNT LEVEL SAS

You can learn more about the account level SAS at <https://learn.microsoft.com/en-us/rest/api/storageservices/create-account-sas>.

Use user delegation SAS

You can also create user delegation SAS using Microsoft Entra ID credentials. The user delegation SAS is only supported by Blob Storage, and it can grant access to containers and blobs. Currently, SAS is not supported for user delegation SAS.

NEED MORE REVIEW? USER DELEGATION SAS

You can learn more about the user delegation SAS at <https://learn.microsoft.com/en-us/rest/api/storageservices/create-user-delegation-sas>.

Configure stored access policies

A SAS token incorporates the access parameters (start and end time, permissions, and so on) as part of the token. The parameters cannot be changed without generating a new token, and the only way to revoke an existing token before its expiry time is to regenerate the storage account key used to generate the token or to delete the blob. In practice, these limitations can make standard SAS tokens difficult to manage.

Stored access policies allow the parameters for a SAS token to be decoupled from the token itself. The access policy specifies the start time, end time, and access permissions, and the access policy is created independently of the SAS tokens. SAS tokens are generated that reference the stored access policy instead of embedding the access parameters explicitly.

With this arrangement, the parameters of existing tokens can be modified by simply editing the stored access policy. Existing SAS tokens remain valid and use the updated parameters. You can revoke the SAS token by deleting the access policy, renaming it (changing the identifier), or changing the expiry time.

NOTE STORED ACCESS POLICY EFFECT

It can take up to 30 seconds for a stored access policy to take effect, and users might see an HTTP 403 when attempting access during that time.

Figure 2-13 shows the creation of stored access policies in the Azure portal.

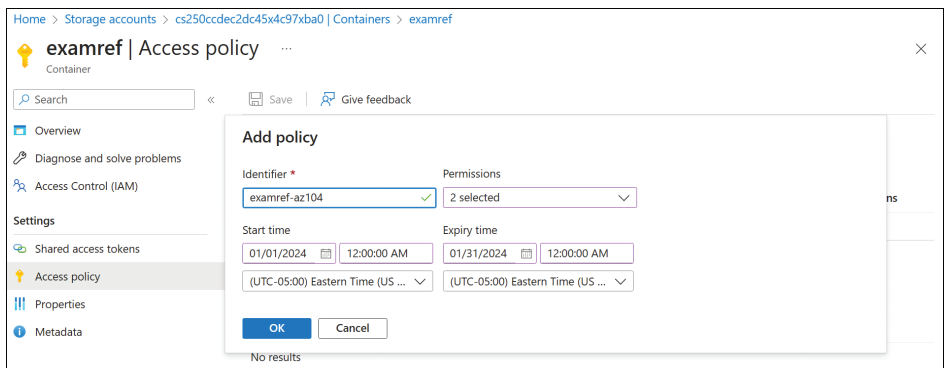


FIGURE 2-13 Creating stored access policies using the Azure portal

Figure 2-14 shows stored access policies being created in Azure Storage Explorer.

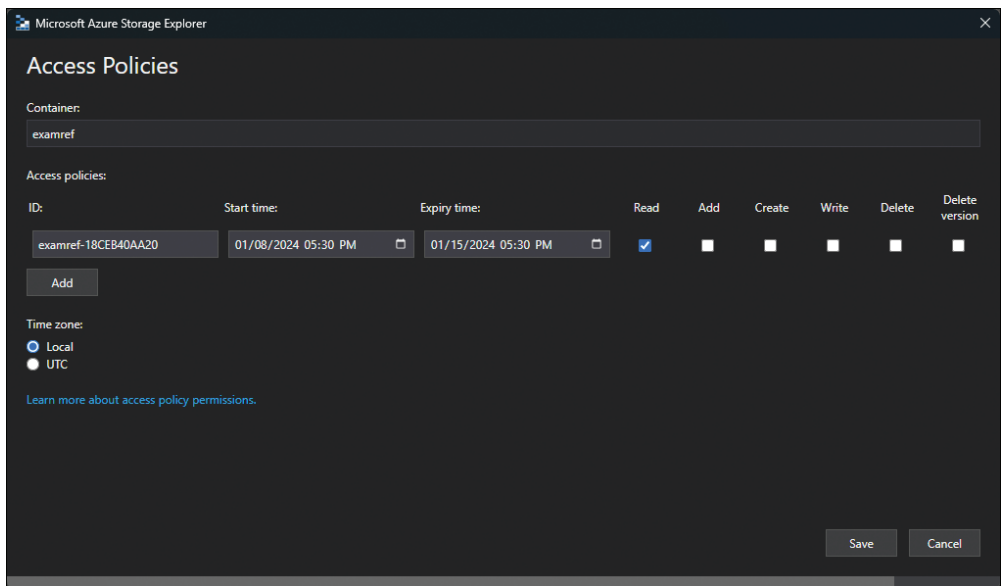


FIGURE 2-14 Creating stored access policies using Azure Storage Explorer

To use the created policies, reference them by name when creating a SAS token using Storage Explorer or when creating a SAS token using PowerShell or the CLI tools.

NOTE MAXIMIUM ACCESS POLICIES

You can have a maximum of only five access policies on a container, table, queue, or file share.

Manage access keys

The simplest way to manage access to a storage account is to use access keys. With the storage account name and an access key to the Azure storage account, you have full access to all data in all services within the storage account. You can create, read, update, and delete containers, blobs, tables, queues, and file shares. In addition, you have full administrative access to everything other than the storage account itself. (You cannot delete the storage account or change settings on the storage account, such as its type.)

Applications will use the storage account name and key for access to Azure Storage. Sometimes, this is to grant access by generating a SAS token, and sometimes, it is for direct access with the name and key.

To access the storage account name and key, open the storage account from within the Azure portal and click Access Keys. Figure 2-15 shows the primary and secondary access keys for a storage account.

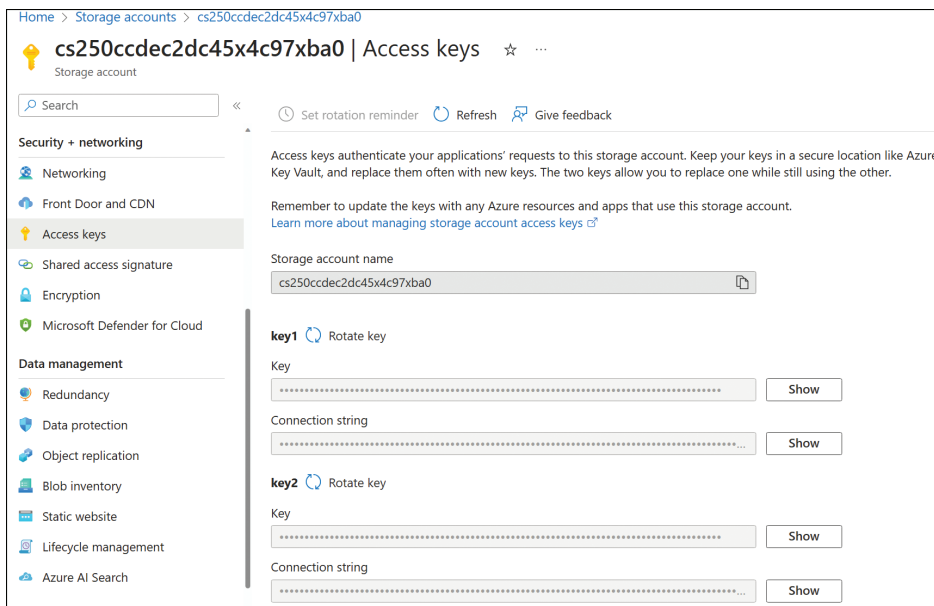


FIGURE 2-15 Access keys for an Azure storage account

Each storage account has two access keys. This means you can modify applications to use the second key instead of the first and then regenerate the first key. This technique is known as “key rolling” or “key rotation.” You can reset the primary key with no downtime for applications that directly access storage using an access key.

Storage account access keys can be regenerated using the Azure portal or the command-line tools. In PowerShell, this is accomplished with the `New-AzStorageAccountKey` cmdlet; with Azure CLI, you will use the `az storage account keys renew` command.

NOTE ACCESS KEYS AND SAS TOKENS

Regenerating a storage account access key will invalidate any SAS tokens that were generated using that key.

Managing access keys in Azure Key Vault

It is important to protect the storage account access keys because they provide full access to the storage account. Azure Key Vault helps safeguard cryptographic keys and secrets used by cloud applications and services, such as authentication keys, storage account keys, data encryption keys, and certificate private keys.

Keys in Azure Key Vault can be protected in software or by using hardware security modules (HSMs). HSM keys can be generated in place or imported. Importing keys is often referred to as bring your own key, or BYOK.

NEED MORE REVIEW? USING HSM-PROTECTED KEYS FOR AZURE KEY VAULT

You can learn more about the bring your own key (BYOK) scenario here:

<https://learn.microsoft.com/en-us/azure/key-vault/keys/hsm-protected-keys>.

Accessing and unencrypting the stored keys is typically done by a developer, although keys from Key Vault can also be accessed from ARM templates during deployment.

NEED MORE REVIEW? ACCESSING ENCRYPTED KEYS FROM AZURE KEY VAULT

You can learn more about how developers securely retrieve and use secrets from

Azure Key Vault here: <https://learn.microsoft.com/en-us/azure/storage/blobs/storage-encrypt-decrypt-blobs-key-vault?tabs=roles-azure-portal%2Cpackages-dotnetcli>.

Configure identity-based access

Microsoft Entra ID authentication is beneficial for customers who want to control data access at an enterprise level based on their security and compliance standards. Entra ID authentication provides identity-based access to Azure storage in addition to existing shared-key and SAS token authorization mechanisms for Azure Storage (Blob and Queue). Azure blobs, files, and queues are supported by Entra ID authentication.

Entra ID authentication enables customers to leverage RBAC in Azure for granting the required permissions to a security principal (users, groups, and applications) down to the scope of an individual blob container or queue. While authenticating a request, Entra ID returns an OAuth 2.0 token to security principal, which can be used for authorization against Azure Storage.

Index

A

- ACA (Azure Container Apps), 123
 - connecting to, 184–186
 - creating an instance, 178–184
 - provisioning a container, 178
 - scaling and sizing, 187–189
- access control, 16
 - blob storage, 77–78, 86–88
 - role-based, 16–19
 - scope, 18–19
- access keys, storage account, 83–84
- access tiers, Azure Blob Storage, 69–70, 110–112
- accountability, organizational, 55
- ACI (Azure Container Instances), 123
 - connecting to, 177–178
 - creating, 174–177
 - scaling and sizing, 186–187
- ACR (Azure Container Registry), 168
 - Access Keys blade, 172
 - creating an instance from the Azure portal, 170–171
 - managing, 172
 - tiers, 169
- action groups, 316–318
- activity logs, 304–305
- additive model, 16–17
- ADFS (Active Directory Federation Services), 1
- administrator role
 - permissions, 49–50
 - subscription, 49
- agents, Log Analytics workspace, 301
- AKS (Azure Kubernetes Service), 123
- alert/s, 311–312
 - action groups, 316–318
 - analyzing across subscriptions, 319–321
 - Azure Monitor, 294
 - budget, 57
 - creating, 312–313
 - rules, 298, 313–315
 - target resource, 313
 - viewing, 318–319
- algorithm, spreading, 168
- alias record, 269–270
- aligned availability set, 163
- allocation, public IP address, 228–229
- App Service, 189–190, 199–200
 - backup, 204–205
 - creating, 193–196
 - deployment slots, 210–211
 - managed certificates, 200–201
 - mapping to a custom DNS name, 196–199
 - network settings, 205–206
 - private key certificates, 201–203
 - public key certificate, 203
- App Service plan
 - creating, 190–192
 - provisioning, 190
 - scaling, 192–193
- append blob, 66, 107
- application, three-tier architecture, 246
- Application Insights, configuration, 321–323. *See also* Azure Monitor, insights
- applying, resource tags, 41
- architecture, three-tier application, 246
- archive access tier, Azure Blob Storage, 69–70
- ARM (Azure Resource Manager) template, 16, 124
 - for adding a public IP address, 128–129
 - Complete mode, 131–132
 - for creating a network interface, 127
 - for creating a virtual network, 126–127
 - for defining a virtual machine resource, 129
 - deployment, 133–135, 137
 - editing, 133–134
 - elements, 125
 - exporting from a deployment, 137–139
 - functions, resourceGroup(), 126
 - Incremental mode, 132
 - modifying an existing, 131
 - parameters, 136, 137
 - UI, 135
 - validation, 135
 - variables, syntax, 126
- ASG (application security group), 246–247, 251–253
- assigned group, 5
- async blob copy, 100–101
- authentication, 84–85, 86–88
- availability, 161
 - set
 - storage account replication mode, 89–91
 - zone, 159–160
- az deployment group create command, 142
- AZ-104 Microsoft Azure Administrator exam, 358–359
 - updates, 358–359
- azcopy command, 99–100
- AzNetworkWatcherNextHop cmdlet, 329

AzureResourceGroupDeployment cmdlet, 137

Azure AD, 1

Azure Backup service, 292, 344–348

Azure Bastion, 255–258

Azure Blob Storage. *See also* blob/s
access tiers, 69, 70, 110–112

Azure CLI (command-line interface), 3

Azure Cost Management, 59–60

Azure Files, 101
automatically reconnect after reboot in Windows, 106
connect and mount from Linux, 106
connect and mount with the net use command, 105
connect and mount with Windows File Explorer, 104–105
connect to Azure files outside of Azure, 103
create a file share, 102–103

Azure Key Vault, 95
managing access keys, 84
pricing, 151

Azure Load Balancer, 263, 277
backend configuration, 279
configuration, 281–286
frontend IP configuration, 278–279
health probes, 279–280
NSG configuration, 281
pricing tiers, 277–278
rules, 280–281
troubleshooting, 286

Azure Monitor, 292–293. *See also* data collection;

Log Analytics; metrics; monitoring
agent ports and protocols, 304
alert/s, 294, 311–312
comparing metrics and logs, 293
insights
logs, 299
metrics, 294–295

Azure Policy, 31, 51. *See also* policy/ies
management groups, 33
policy compliance, 37–38
policy definitions, 33–34

resource groups, 33
scoping, 33

Azure portal, 3
Add Peering blade, 225–227
App Service, changing the network settings, 206–209
App Service, creating, 193–196
ARM template
ASG (application security group), configuration, 251–253
authoring queries, 308–309
Azure Load Balancer
configuration, 281–286
Azure Policy Assign Initiative blade, 37
Azure Policy Assignments blade, 36
Azure Policy Definitions blade, 34
bulk operations, 8–9
containers, managing, 107–109. *See also* container/s
Create a Storage Account blade, 71–73
Create a Virtual Machine blade
Create Container Instance blade, 174–175
Create Container Registry blade, 170
Create Virtual Network blade, 219–221
custom DNS configuration, 274–275
custom role, creating, 20–25
Effective Security Rules view, 253–254
file share, creating, 102–103
group
guest users, managing, 10–12
IAM blade, 26
Metrics blade, 296–298. *See also* metrics
Move Resources blade, 154
Notifications blade, 15
NSG (network security group), creating, 247–249
policy definitions, creating, 33–37
public IP address, creating, 231–232

Registration blade, 14–15
role assignments, managing, 25–28
SAS token, creating, 78–79
SSPR (self-service password reset), 14
storage account, creating, 70–74
UDR configuration, 236–238
users, creating, 3
Users blade, 3
VMSS (Virtual Machine Scale Set), creating, 164–165
Azure Site Recovery, configuration, 335–343
Azure Storage, 65
Azure Storage Explorer, 95
connecting to storage accounts, 96–99
copying between storage accounts, 99
creating an SAS token, 80
Azure subscription, 29

B

backup and recovery, 331
App Service, 204–205
Azure Backup service, creating, 344–348
Azure Site Recovery, 335–343
backup policy, 348–351
Recovery Services vault, 332–333
restoring a VM, 346–348
soft delete, 113–115, 333–335
backup report, 351–353
BCDR (business continuity and disaster recovery) plan, 335
Bicep, 140
code, 140–141
file
installing the tools, 141
billing, subscription, 58
blob/s, 66, 110–112
access control, 77–78
block, 66, 107. *See also* VNet (virtual network)
containers, 106–107
copying, 99, 100–101

blob/s, continued

- Entra ID authentication, 86–88
- lifecycle management, 117–119
- object replication, 91–95
- RBAC roles, 85
- resource scope, 85–86
- types, 107
- user delegation SAS (shared access signature), 81
- versioning, 115–116
- bring your own DNS, 273–274
- budget
 - alerts, 57
 - creating, 55
 - subscription, 55
 - threshold, 55
 - viewing, 57
- built-in policy, 32
- built-in role, 17–18, 20, 25, 50
- bulk operations, 9
- BYOD (bring-your-own-device), 12

C

- certificate
 - managed, 200–201
 - private key, 201–203
 - public key, 203
- chart
 - adding metrics, 296–298
 - line, 298
 - query-based, 310
- child DNS zone, 268
- CIDR (classless inter-domain routing), 216, 220
- cloning, built-in role, 20, 25
- cloud-only users, 3
- cmdlet/s, 55
 - AzNetworkWatcherNextHop, 329
 - AzResourceGroupDeployment, 137
 - Get-AzNetworkWatcherTopology, 331
 - New-AzResourceGroupDeployment, 142
 - New-AzStorageAccountKey, 83
 - Test-AzNetworkWatcherIPFlow, 328

- code, 124
 - Bicep, 140–141
 - infrastructure as, 131, 140
- cold access tier, Azure Blob Storage, 69
- commands
 - az deployment group create, 142
 - azcopy, 99–100
 - Docker, registryname.azurecr.io, 172
 - mount, 106
 - net use, 105
 - query, 308
- Complete mode, ARM (Azure Resource Manager)
- template, 131–132
- compliance, policy, 37–38
- compute resources, 123
- configuration
 - Application Insights, 321–323
 - ASG (application security group), 251–253
 - Azure Load Balancer, 281–286
 - Azure Site Recovery, 335–343
 - DNS, 270–273
 - Entra ID Join, 12–14
 - Log Analytics workspace, 299–304
 - public IP address, 227
 - SSPR (self-service password reset), 14–15
 - storage
 - UDRs (user-defined routes), 236–238
- Connection Monitor, 240–241
- Connection Troubleshoot, 239–240
- container/s, 123, 168. *See also* ACA (Azure Container Apps); ACI (Azure ContainerInstances); ACR (Azure Container Registry)
 - blob, 106–107
 - management
- cool access tier, Azure Blob Storage, 69
- copying, between storage accounts, 99, 100–101
- cost center quota, 55–57
- cost management, 53–54, 58–60
- creating
 - ACI (Azure Container Instances), 174–177

- alerts, 312–313
- App Service, 193–196
- App Service plan, 190–192
- availability set, 161–163
- Azure Backup service, 344–348
- Azure Bastion service, 255–258
- budget, 55
- file share, 102–103
- groups, in Azure portal, 4
- NSG (network security group), using Azure portal, 247–249
- policy definitions, 33–37
- queries, 307–309
- Recovery Services vault, 332–333
- resource locks, 39
- role/s
- SAS (shared access signature)
- token
- storage account
- stored access policy, 82
- subnets, 220–221
- users
 - VM (virtual machine), 144–145.*See also* Azure portal, Create a Virtual Machine blade
 - VMSS (Virtual Machine Scale Sets), 164–165
 - VNet (virtual network), 219–221
- custom role
 - assignable scopes, 23
 - creating, 20–25
 - permissions, 21–23

D

- dashboard, 298
 - Application Insights, 322–323
 - Azure Monitor Alerts, 320
 - saving queries to the, 309
- data backup and recovery
 - snapshots, 115–116
 - soft delete, 113–115
 - versioning, 115–116
- data collection, 299–300
 - adding a data source destination, 303–304
 - resources, 301–302
 - rules, 300–301
- default rules, NSG, 245

- definition
 - initiative, 31
 - policy, 31–32, 33–37
- Delete lock, 38
- deleting
 - devices, 8
 - Entra ID directories, 29
 - resource groups, 46–48
- deny assignment, 19
- dependency, 127, 128
- deployment
 - ARM template, 133–135, 137
 - Bicep file, 142
 - exporting a template from, 137–139
 - Network Watcher, 327
 - slots, 210–211
 - VM (virtual machine), 143–144
- development
 - Application Insights, 321–323
 - containers and, 168
 - Entra ID, 1
- device
 - associating with Entra ID, 12
 - deleting, 8
 - hybrid Entra join, 14
 - identity, 12
 - managed, 12
 - management, 7–8
 - non-hybrid Entra join, 14
 - registration, 12–13
- diagnostic logs, 304, 305–307
- directories, Entra ID, 28, 29
- disabling, VM encryption, 153
- disks
 - managed, 163
 - storage, 66
 - VM (virtual machine), managing, 158–159
- DMZ (demilitarized zone), 215–216
- DNS
 - alias record, 230
 - bring your own, 273–274
 - CNAME record, 230
 - custom settings, 272–273, 274–275
 - labels, 229–230
 - local, 264
 - name resolution, 262, 264–265

- A record, 230
- records, 268–269
- resolution VNet, 275
- reverse lookup, 265
- server, 274
- services, 266
- zone, 263–264
- Docker, registryname.azurecr.io
- command, 172
- Docker Hub, 168
- dynamic allocation, public IP
- address, 228
- dynamic group/s, 5–6

E

- EA (Enterprise Agreement), 58, 59
- editing
 - ARM template, 133–134
 - groups, 6
- Effective Security Rules view, Azure portal, 253–254
- encryption
 - storage account, 95–96
 - VM (virtual machine)
- endpoints
 - health probes, 280
 - private, 259–262
 - service, 258
- Entra Admin Center, 3, 8–9
- Entra Connect, 1
- Entra Connect Sync, 1
- Entra External ID, 1
- Entra ID, 1
 - authentication, 84–85, 86–88
 - cloud-only users, 3
 - development, 1
 - Device Settings blade, 12–13
 - directories, 28, 29
 - Join, configuration, 12–14
 - license/s
 - roles, 18
 - SSPR (self-service password reset), 14–15
 - subscription, 48
 - tenant, 28
- Entra ID B2B, 1
- external users, managing, 10–12

F

- fault domain, 163, 168
- file share, creating, 102–103
- files
 - Bicep
 - storage, 66
- firewall, storage, 74
 - access from trusted Microsoft services, 75
 - address space, 75
 - configuration, 74
- forced tunneling, 236
- Function App, 316
- functions
 - ARM template, 125
 - resourceGroup(), 126

G

- geo-replications, 174
- Get-AzNetworkWatcherTopology cmdlet, 331
- global peering, 222
- governance, subscription, 50–51
- graphs, query-based, 310
- group/s, 4. *See also* ASG (application security group); NSG (network security group)
 - action, 316–318
 - assigned, 5
 - creating, in Azure portal, 4
 - dynamic, 5–6
 - editing, 6
 - management, 6, 18, 33, 50–53
 - Microsoft 365, 5
 - placement, 163–164
 - properties, 6–9
 - RBAC (role-based access control), 17
 - resource, 30, 33
 - security, 5
- GRS (geographically redundant storage), 68
- Guest OS metrics, 295–296
- guest users, managing, 10–12
- GZRS (geographically zone redundant storage), 68

H

- health monitoring, VMSS (Virtual Machine Scale Sets), 166–167
- health probes, Azure Load Balancer, 279–280
- hierarchy, management group, 51
- hot access tier, Azure Blob Storage, 69
- HSM (hardware security module), 84
- hub-and-spoke topology
 - creating a VNET peering on, 225–227
 - VNet, 223
- hybrid Entra join, 14
- hybrid Entra joined devices, 14

I

- identity, 1, 12
- inbound NAT rule, 280–281
- Incremental mode, ARM (Azure Resource Manager) template, 132
- infrastructure
 - as code, 131, 140
 - as-a-service, 291
- inheritance, 18, 38
- initiative definition, 31
- insights
 - network, 325–326
 - storage account, 325–326
 - VM (virtual machine), 323–325
- installing, Bicep tools, 141
- IP Flow Verify, 327–328
- IP forwarding, 235
- IP range
 - subnet, 217
 - VNet, 216–217
- ITSM (IT Service Manager), 316

J-K

- JSON (JavaScript Object Notation), 25
 - ARM template, 124
 - schema file, 125

- key rolling, 83
- KQL (Kusto Query Language), 307–308, 309

L

- large scale set, 164
- LDNS (local DNS), 264
- legacy storage account types, 67–68
- license, Entra ID
 - management, 10
 - purchasing, 10
 - SSPR requirements, 14
- line chart, 298
- Linux, 106
- load balancing, 277. *See also* Azure Load Balancer
 - inbound NAT rule, 280–281
 - logs, 286
 - troubleshooting, 286
- lock/s
 - inheritance, 38
 - resources, 38
- Log Analytics, 293
 - data collection
 - pricing, 299, 300
 - querying, 294, 307–309
 - workspace
- logs
 - activity, 304–305
 - Azure Monitor, 293
 - diagnostic, 304, 305–307
 - load balancer, 286
 - querying, 307–309
- LRS (locally redundant storage), 68

M

- managed certificate, 200–201
- managed disks, 163
- management
 - ACR (Azure Container Registry)
 - container
 - cost, 53–54
 - device, 7–8
 - external user, 10–12

- group, 6–7, 18, 50–53
- license, 10
- plane, 38–39
- resource group, 41–42
- subscription, 48–49
- VM disk, 158–159
- method, validateMoveResources, 44–45
- metrics, 294–295, 304. *See also* data collection
 - Azure Monitor, 293
 - multidimensional, 296
 - one-dimensional, 296
 - populating a chart, 296–298
 - properties, 296
 - retention period, 295–296
 - and visual response times, 299
- Microsoft 365, 1, 5
- Microsoft Entra ID. *See* Entra ID
- Microsoft Graph, 3
- modifying an existing ARM template, 131
- monitoring
 - health, VMSS, 166–167
 - resource costs, 58–60
- mount command, 106
- move operations
 - resource group, 42–46, 153–156
 - support, 43
- multidimensional metrics, 286, 296

N

- name resolution, 262, 264–265
- name server, 267
- naming conventions
 - storage account, 66
 - subnet, 217
- net use command, 105
- network insights, 325–326
- network interface, 127
- network topology view, 330–331
- Network Watcher, 327
 - Connection Monitor, 240–241
 - Connection Troubleshoot, 239–240
 - deployment, 327
 - IP Flow Verify, 327–328

- network topology view, 330–331
- Next Hop, 328–329
- Packet Capture, 329–330
- New-AzResourceGroupDeployment cmdlet, 142
- New-AzStorageAccountKey cmdlet, 83
- Next Hop, 328–329
- NIC (network interface card), associating an NSG, 249–251
- non-hybrid Entra join, 14
- notifications, 15
- NSG (network security group), 242
 - applying to VNets, 248–249
 - associating to a subnet or network interface, 249–251
 - configuring on Azure Load Balancer, 281
 - creating with Azure portal, 247–249
 - rules, 242–243, 253–254
- NVA (network virtual appliance), 224–225

O

- object replication, 91–95
- one-dimensional metrics, 296
- optimization, resource, 291–292
- organizational accountability, 55

P

- PaaS (platform as a service), 258
- Packet Capture, 329–330
- page blob, 66, 107
- parameters, ARM template, 125, 137
- passwords, self-service reset, 14–15
- peering, VNet, 222
 - creating with Azure portal, 225–227
 - global, 222
 - requirements and constraints, 222
- performance tier, storage account, 67

- permissions, 17
 - administrator role, 49–50
 - custom role, 21–23
- placement group, 163–164
- planning, resource tagging
- taxonomy, 40–41
- policy/ies
 - Azure, 31
 - backup, 348–351
 - built-in, 32
 - compliance, 37–38
 - definition, 31–32, 33–37
 - management groups, 33
 - replication, 337–338
 - scoping, 33
 - stored access, 81–82
 - upgrade, 166
- port mapping, 281
- POST request, move operation, 44
- PowerShell
 - cmdlet/s, 55, 108
 - runbook, 316
- precedence rules, route table, 235–236
- Premium tier, storage account, 67
- pricing
 - Azure Key Vault, 151
 - Azure Load Balancer, 277–278
 - Log Analytics, 299, 300
 - public IP address, 227–228
- principles of least privilege, 17
- private DNS zone, 275–277
- private endpoints, 259–262
- private key certificates, 201–203
- property/ies
 - DNS label, 230
 - DNS record, 268
 - group, 6–9
 - metric, 296
 - NSG (network security group), 242–243
 - user, 6–9
 - VNet (virtual network), 218
- public IP address
 - adding to VM, 128–129
 - configuration, 227
 - creating with Azure portal, 231–232
 - DNS labels, 229–230
 - dynamic allocation, 228

- outbound internet connections, 230–231
- prefix, 229
- pricing tiers, 227–228
- static allocation, 228–229
- public key certificate, 203
- purchasing, Entra ID license, 10

Q

- queries/querying
 - creating charts and graphs from, 310
 - Log Analytics, 294, 307–309
 - saving to the dashboard, 309
 - scope, 308
 - table-based, 308
- queues
 - RBAC roles, 85
 - resource scope, 85–86
 - storage, 66
- quota
 - cost center, 55–57
 - request, 54–55
 - resource, 44, 53, 54–55
 - spending, 59

R

- RA-GRS (read access geographically redundant storage), 68
- RA-GZRS (read access geographically zone redundant storage), 68
- RBAC (role-based access control), 1, 16–19, 31
 - access assignments, 25–28
 - additive model, 16–17
 - and management groups, 53
 - role/s, 16, 18
 - scope, 18–19
- Read-only lock, 38, 39
- records
 - alias, 269–270
 - DNS, 268–269, 270–273
 - SPF, 269

Recovery Services vault

- Recovery Services vault, 332
 - creating, 332–333
 - soft delete, 333–335
- recursive DNS server, 264–265
- registration, device, 12–13
- registryname.azurecr.io command, 172
- removing
 - resource groups, 46–48
 - role assignment, 28
 - subnets, 217
- replication
 - object, 91–95
 - policy, 337–338
 - from source VM, 336–343
 - storage account, 68–69, 89
- report
 - backup, 351–353
 - resource cost, 58–60
 - usage, 40
- request, quota, 54–55
- resolution VNets, 275
- resourceGroup() function, 126
- resource/s, 29, 30. *See also* metrics;
- VM (virtual machine)
 - additive model, 16–17
 - compute, 123
 - cost management, 58–60
 - data collection, 301–302
 - dependency, 127
 - groups, 30, 33
 - ID, 156, 226–227
 - lock/s, 38
 - optimization, 291–292
 - permissions, 17
 - policy definition, 31–32
 - provider, 43–44
 - public IP address, 227
 - quota, 44, 53, 54–55
 - role inheritance, 16
 - scope, 18–19, 85–86
 - tags, 40, 54
 - target, 313
- restoring a recovery point, 346–348
- retention period, metrics, 295–296
- reverse DNS lookup, 265
- role/s, 16
 - administrator, permissions, 49–50
 - assignment, 17–19, 25–26
 - built-in, 17–18, 50

- cloning, 25
- custom
 - definition, 17
- Entra ID, 18
- inheritance, 16, 18
- RBAC (role-based access control), 18
- route table, 233–234
 - creating, 236
 - precedence rules, 235–236
- rules
 - alert, 294, 298, 313–315
 - Azure Load Balancer, 280
 - data collection, 300–301
 - lifecycle management, 117–119
 - NSG (network security group), 242–243, 253–254
 - object replication, 92–94
 - precedence, 235–236
 - scale, 189
 - VMSS management, 166
- runbook, 316

S

- SAS (shared access signature), 78
 - token, creating
 - URI, 80–81
 - user delegation, 81
- saving authored queries to the dashboard, 309
- scale set, 163–164
- scaling and sizing
 - ACA (Azure Container Apps), 187–189
 - ACI (Azure Container Instances), 186–187
 - App Service plan, 192–193
- scope/s, 18–19
 - Azure Cost Management, 60
 - deny assignment, 19
 - management group, 51–52
 - policy, 33
 - query, 308
 - resource, for blobs and queues, 85–86
- security
 - group, 5, 17. *See also* NSG (network security group)
 - principal, 19
- server
 - DNS, 274
 - name, 267
 - recursive DNS, 264–265
- service/s. *See also* subscription
 - Azure Bastion, 255–258
 - chaining, 224–225
 - DNS, 266
 - endpoints, 258
 - infrastructure-as-a-, 291
 - private endpoints, 259–262
 - resource/s, 29
 - storage, 66, 74
 - tag, 222–223, 244
- shared VNet gateway, 225
- single sign-on, 12
- size, VM (virtual machine), changing, 156–158
- SMB, 103
- snapshots, 115–116
- soft delete, 113–115, 333–335
- spending limits, Azure subscription, 53–54, 59
- SPF (Sender Policy Framework) records, 269
- spreading algorithm, 168
- SSPR (self-service password reset), 2, 14–15
- stacked bar chart, 310
- Standard tier, storage account, 67
- static allocation, public IP address, 228–229
- storage, 65. *See also* Azure Blob Storage
 - account/s, 65
 - backup and recovery, soft delete, 113–115. *See also* backup and recovery
 - blob/s, 66
 - disks, 66
 - files, 66
 - firewall, 74
 - identity-based access, 84–85
 - queues, 66
 - replication, 89
 - SAS (shared access signature) service, 74
 - snapshots, 115–116
 - tables, 66
 - virtual network service endpoints, 75–76

Storage Explorer, containers, managing, 109
 stored access policy, 81–82
 subnets, 215–216, 217. *See also* VNet (virtual network)

- associating an NSG, 249–251
- creating, 220–221
- IP range, 217
- removing, 217
- route table, 233–234, 235–236
- settings, 218

subscription
 activity logs, 304–305
 administrators, 49
 alerts, 319–321
 Azure, 29
 billing, 58
 budget, 55
 governance, 50–51
 managing, 48–49
 moving resources between, 43–44
 resource groups, 30–31
 resource locks, 38
 spending limits, 53–54
 types, 48
 sync blob copy, 101
 system routes, 231–233, 236

T

table/s
 querying, 308
 storage, 66
 tags
 resource, 40, 54
 service, 222–223, 244

target resource, 313
 template

- ARM, 16, 124, 130–131
- VHD, 132–133

Test-AzNetworkWatcherIPFlow cmdlet, 328
 three-tier application architecture, 246

threshold, budget, 55

tools

- Bicep, installing, 141
- Connection Monitor, 240–241

Connection Troubleshoot, 239–240

Network Watcher. *See also* Network Watcher

topology, hub-and-spoke, 223

troubleshooting

- load balancing, 286
- tools, Connection Troubleshoot, 239–240. *See also* tools

U

UDRs (user-defined routes), 224–225, 233–235, 236–238

UI (user interface), ARM template, 135

upgrade, policy, 166

uploading and downloading data

using azcopy, 100

URI, SAS (shared access signature), 80–81

Usage Location property, 10

usage report, 40

user delegation SAS (shared access signature), 81

user/s

- cloud-only, 3
- creating, bulk operations, 9
- creating, in Azure portal, 3
- guest, managing, 10–12
- profile, 6
- properties, 6–9
- Usage Location property, 10

V

validateMoveResources method, 44–45

vanity name server, 267

variables, ARM template, 125, 126, 129, 135

versioning, 115–116

VHD template, 132–133

viewing

- alerts, 318–319
- budget, 57

virtual network, 126–127

VirtualNetwork service tag, 222–223

VM (virtual machine), 123, 143. *See also* VNet (virtual network)

- adding a public IP address, 128–129

- availability set, 161

- availability zone, 159–160

- backing up, 344–346

- changing the size of, 156–158

- creating, 144–145. *See also* Azure

- portal, Create a Virtual Machine blade

- defining, 129

- deployment, 143–144

- disks, managing, 158–159

- encryption, 150

- insights, 323–325

- IP forwarding, 235

- moving, 153

- network interface, creating, 127

- outbound internet connections, 230–231

- replication, 336–343

- restoring, 346–348

- types, 156–157

VMSS (Virtual Machine Scale Sets), 123, 163

- advanced rules, 167

- creating, 164–165

- health monitoring, 166–167

- placement group, 163–164

- spreading algorithm, 168

- upgrade policy, 166

VNet (virtual network), 210–211, 215–216

- Azure Bastion, 255

- Azure Bastion service, creating, 255–258

- CIDR (classless inter-domain routing), 216, 220

- creating, 219–221

- hub-and-spoke topology, 223

- IP forwarding, 235

- IP range, 216–217

- NSGs, applying, 248–249

- NVA (network virtual appliance), 224–225

- peering, 222

VNet (virtual network), continued

VNet (virtual network), *continued*
 properties, 218
 resolution, 275
 service endpoints, storage and,
 75–76
 shared gateway, 225
 subnets, 217
 system routes, 231–233
 UDRs (user-defined routes),
 224–225, 233–235
 VPN, forced tunneling, 236

W

webhooks, 173, 316–317
Windows, non-hybrid Entra join, 14
Windows File Explorer, mapping a
network drive to an Azure file share,
104–105
workspace, Log Analytics
 agents, 301
 configuration, 299–304

X-Y-Z

zone, DNS, 263–264
 child, 268
 configuration, 270–273
 delegating to Azure DNS,
 266–268
 private, 275–277
ZRS (zone redundant storage), 68